REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, Claim 24 has been amended. No claims have been cancelled or added by this amendment. Hence, Claims 24-36, and 51-58 are pending in the Application. It is respectfully submitted that the amendments to the claims as indicated herein do not add any new matter to this application. Furthermore, amendments made to the claims as indicated herein have been made to improve readability and clarity of the claims.

Each issue raised in the Office Action mailed February 2, 2004 is addressed hereinafter. It is respectfully submitted that the rejection of Claims 24-36 and 51-58 as amended are over come for reasons given hereafter.

SUMMARY OF REJECTIONS/OBJECTIONS

In the Office Action, Claims 51 and 52 are rejected under 35 U.S.C. 112, first paragraph because the specification for Claims 51-58 it does not reasonably provide enablement for "a tamper-resistant mechanism for storing one or more keys," or provide enablement for "a tamper-resistant non-volatile card."

Claims 24, 26, 28, 29, and 36 are rejected under 35 U.S.C. 102(b) as being anticipated by Netscape Proxy Server Administrator's (N.P.S.A.) Guide.

Claims 25, 27, 30, 31, 32, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Netscape Proxy Server Administrator's Guide in view of Bellwood (WO 01/03398 A2).

Claims 37, 52, 53, 54, 55, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Netscape Proxy Server Administrator's Guide in view of Maruyama et al. (US2002/0015497 A1).

Claims 56 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Netscape Proxy Server Administrator's (N.P.S.A.) guide in view of Maruyama et al. (US2002/0015497 A1) in further view of Bellwood (WO 01/03398 A2).

REJECTIONS UNDER 35 U.S.C. § 112

CLAIMS 51 and 52

In the Office Action, Claims 51 and 52 are rejected under 35 U.S.C. §112, first paragraph. The Office action states that the specification does not reasonably provide enablement for "a tamper-resistant mechanism for storing one or more keys" and for "a tamper-resistant non-volatile card."

The specification provides support for tamper-resistant mechanisms. For example, on page 8, lines 22-33 and page 9, lines 1-2, the specification states that, "[t]o ensure the information remains secure, information is stored on non-volatile mediums encrypted under a separate key known only to the server. The server maintains the key to the information using a tamper resistant non-volatile card."

CLAIM 24

Claim 24, as amended, recites in part:

"encrypting said content using the first secure session protocol for sending, using the first session, to the at least one web browser in response to the encrypted request for content;
encrypting the requested content using a third secure session protocol for storing the encrypted requested content locally in a memory at the at least one SRP; and
retrieving the content from the memory at the at least one SRP upon subsequent requests for the content."

In the Office Action, it was stated that "figure 7.4 show [*sic*] that whatever information that is being sent from the proxy to the client is encrypted." It is respectfully

submitted that the third session protocol in Claim 24 is NOT for sending encrypted material from the proxy to the client (web browser). Rather, the third session protocol is for encrypting the information with a new key for storage in cache. Such a feature is neither taught nor reasonably suggested in the cited references.

Claim 24, as originally filed, contains the limitation of establishing a first secure session protocol between the secure proxy server (SRP) and the web browser. Thus, since a secure session has already been established between the secure proxy server and the web browser, in the interest of efficiency, it follows that the same established secure session would be used for sending the encrypted material from the secure proxy server to the web browser. Page 8, lines 13-15 of the specification describes the sending of the requested information using the "current SRP/browser session keys", i.e., the already established (first session) keys.

The last paragraph on page 8 of the specification goes on to explain that in order to ensure that the information is stored by the proxy server in a secure fashion, the proxy server uses an entirely "separate key", i.e. a third secure session protocol as required by Claim 24. In the office action, it is stated that the third session protocol is used to encrypt data to be sent to the client. This implies that the client would know the key associated with the third secure session for decrypting the requested data sent from the proxy server. However, the third secure session protocol is known only to the SRP and is separate from the first secure session protocol (between proxy server and client) and separate from the second secure session protocol (between proxy server and web server). Page 8, line 22 to page 9, line 1 of the specification states that "[t]o

ensure the information remains secure, information is stored on non-volatile mediums encrypted under a separate key known only to the server."

As previously explained, the SRP encrypts and sends the requested data to the client using the already established first session protocol known to both the proxy server and the client web browser and not the third secure session protocol. The SRP uses the third secure session protocol for encrypting the information for secure storage in the cache.

The cited references do not disclose encrypting the requested content using a third secure session protocol for the purpose of storing the content in the local memory that is associated with the secure reverse proxy.

Thus, the Netscape Proxy Server Administrator's Guide, whether taken alone, or in combination with *Maruyama* and *Bellwood*, does not disclose, teach or suggest encrypting the requested content using a third secure session protocol known only to the SRP for purposes of securely storing the content in the local cache at the SRP. Thus, Claim 24 is neither anticipated by Netscape Proxy Server Administrator's Guide nor rendered obvious over Netscape Proxy Server Administrator's Guide, whether taken alone or in view of *Maruyama* and *Bellwood*.

CLAIMS 25-36

Claim 25 has the limitation, "the third secure session protocol is known only to the at least one SRP". As previously explained, the novelty is that only the SRP knows the key (third secure session protocol) for encrypting the content before storing the

content in the cache. Such a feature is neither taught nor reasonably suggested in the cited references. Thus, Claim 25 is allowable.

Further, Claims 25-36 are either directly or indirectly dependent upon independent Claim 24, and include all the features of Claim 24. Therefore, it is respectfully submitted that Claims 25-36 are allowable for at least the reasons provided herein with respect to Claim 24.

CLAIMS 51-58

The novelty in Claim 51 is the limitation that "the one or more keys are known only to the SRP and are used for encrypting the content before storing the content in a secure local cache for future requests for the content." None of the cited references disclose or suggest such a limitation. Please refer to the arguments proffered herein in respect to Claim 24 for a more detailed explanation.

Claims 52-58 are either directly or indirectly dependent upon independent Claim 51, and include all the features of Claim 51. Therefore, it is respectfully submitted that Claims 52-58 are allowable for at least the reasons provided herein with respect to Claim 51.

CONCLUSION

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

If in the opinion of the Examiner a telephone conference would expedite the prosecution of the subject application, the Examiner is encouraged to call the undersigned at (650) 838-4311.

The Commissioner is authorized to charge any fees due to Applicants' Deposit Account No. 50-2207.

Respectfully submitted,
Perkins Coie LLP

Date: June 1, 2004

Carina M. Tan
Registration No. 45,769

Correspondence Address:

Customer No. 22918
Perkins Coie LLP
P. O. Box 2168
Menlo Park, California 94026
(650) 838-4300